

Prepare Now for the End of Windows XP and Office 2003 Support in Less Than a Year

Published: 8 April 2013

Analyst(s): Michael A. Silver, Stephen Kleynhans

Microsoft will end support for Windows XP and Office 2003 in less than a year. IT leaders and endpoint computing managers must ensure that they will either be off these products, or that they have considered the risks of continuing to run them.

Key Findings

- Microsoft support for Windows XP and Office 2003 will end on 8 April 2014, and Gartner does not believe Microsoft will extend this date.
- After Microsoft ends support for these products, organizations can purchase Custom Support from Microsoft, which is relatively expensive (usually \$200,000 minimum, and we've seen multimillion dollar contracts).
- Organizations are usually less worried about running a version of Office without support, but most want to avoid running a version of Windows without support.

Recommendations

- Understand the risks that lack of support for these products will bring to your organization.
- Prioritize your users and applications, and move the most critical ones to supported platforms first, if possible.
- Address users and applications that can't be migrated off Windows XP or Office 2003 with other means to reduce risk (additional security, isolation, etc.).

Strategic Planning Assumption

By 2014, more than 15% of midsize and large enterprises will still have Windows XP running on at least 10% of their PCs after Microsoft support ends.

Analysis

As the end of Windows XP support by Microsoft nears, we still get questions from organizations that are in the early stages of migration, or have not even started migrating off the platform. At the very least, organizations should now assess their systems and the risks they will be open to if they do not migrate to supported platforms. Most organizations will need to take action to reduce the risk for at least some users and/or applications.

Understand the Risks Involved

Microsoft supports its products for at least 10 years. For the first five years, the product is in Mainstream Support, and Microsoft will fix any problems. For the next five years, the product is in the Extended Support phase, and Microsoft will only fix security vulnerabilities. Support inquiries can be submitted during the entire 10-year life of the product.

The end of Extended Support marks the end of free technical support to the masses. After that, only organizations that sign up for Custom Support will get security fixes. Custom Support is a relatively expensive offering that costs \$200 per PC per year for the first year (payable quarterly), with a minimum cost of \$200,000 (regardless of the number of PCs; see "Custom Support Will Be Available for Windows XP at a Price"). No third party can offer the same level of support, because only Microsoft has and can fix the source code.

Not getting fixes means that organizations' PCs could be vulnerable to attack. New vulnerabilities are always being found, and new vulnerabilities that are found in more current products could affect Windows XP and Office 2003. Any unpatched device can be vulnerable to attack. Even if a device is only a private network and has no Internet access, another device, even one running a supported product, can be infected with malware outside the private network and can bring it onto the private network, infecting other devices.

Furthermore, many applications will no longer be supported while running on Windows XP. Organizations may be on their own to resolve issues and problems, which could result in system downtime.

The amount of risk organizations perceive depends on various internal factors and product issues. Organizations in the financial services industry generally believe they are at a higher risk than those in manufacturing. Many organizations look at the relatively few broad vulnerabilities and attacks on Office, and decide that leaving some users on the unsupported product will have a very low risk. However, more serious vulnerabilities often are found in versions of Windows, and most organizations take significant steps to lower the risk by moving off Windows XP, adding security or hardening products and processes to reduce the surface area for attack, or improving PC lockdown using other means to reduce the chance of attack and the damage attackers can do.

Assess Your Position

Organizations that are not almost or completely finished migrating off Windows XP and/or Office 2003 should reassess their position by reviewing their project plans and ensuring that they are on target to meet the deadline. Organizations that believe they're unlikely to complete their migration

projects by April 2014 should prioritize their applications and users so that they can reduce the risks by addressing critical resources first.

Classify Applications and Users — Work on Critical Ones First

Most organizations have far too many applications. Organizations where users are administrators typically have one application for every 10 users, with about half of these requiring Windows to run. Gartner defines a critical application (or the user of critical applications) as one where if the application fails or the user can't do his or her job, there could be financial or legal consequences.

Organizations must conduct several analyses on their application portfolios to help safeguard the organization after XP support ends, and in preparation for Windows 7 or 8 migrations:

- Inventory the software installed on user PCs.
- Meter application usage, and compare this with the installed-software list.
- Identify other low-use or duplicative applications.
- Work with users and business managers to reduce the number of applications used in the organization.
- Work with users and business managers to classify applications by criticality.
- For critical applications, decide whether official vendor support is needed/desired before Windows 7 can be deployed, and find out if there is a supported version.

For critical applications that can run on Windows 7, consider moving these users first. If Windows 7 can't be used, prioritize these applications and users so that you can move them as soon as possible.

Classify users and/or PCs as critical/less critical, and or more/less vulnerable to external attacks on unpatched systems.

These users should be classified as critical:

- Users with confidential data
- Users in parts of a business that has government regulation or oversight
- Users who are involved in revenue-generating activities whose PCs are open to the Internet
- Users who run applications deemed to be critical

Understand the Problems and Solutions

Organizations have many reasons for not being able to eliminate Windows XP (or Office 2003) by April 2014. Depending on the reason, different actions can be taken to resolve the problem or reduce the risk (see "How to Protect Your PCs If You Are Still Running Windows XP in April 2014"). Organizations that are running late or know they will not be finished in time should determine why

this is so, and should use these tactics to get back on target, or reduce the risk for users and devices that will be running unsupported software.

If the Windows application does not run on Windows 7 (in order of preference):

- Fix, upgrade or replace the application.
- Run the application remotely using server-based computing (SBC; if the application runs in that environment).
- Virtualize the application (although this may not resolve the issue).
- Install a reduced number of isolated Windows XP physical or virtual machines, with limited access or extra security.

If the vendor does not support Windows applications on Windows 7, but it works:

- Test the application, and evaluate the risk.
- Especially for your most critical applications, if the application works, work with your independent software vendor (ISV) to understand its support policies, and decide how important it is to conform to the vendor's requirements.

If the browser application does not work on Internet Explorer (IE) 8 (in order of preference):

- Fix, upgrade or replace the application.
- Have users access the site/application via SBC.
- Investigate other browser compatibility products (e.g., Browsium Ion; see "How HMRC's Use of Browsium Kick-Started Its Move to Windows 7").
- Install a reduced number of isolated Windows XP physical or virtual machines, with limited access or extra security.
- Some organizations are considering virtualizing the required browser on Windows 7. This may work, but organizations should understand that Microsoft considers this a license violation.

If there's not enough time to finish the migration:

- Hire a service provider to help you finish in time.
- Do as many of these as are practical:
 - Reduce the scope of the project (eliminate add-ons).
 - Revisit the business case to understand the cost and risk of remaining on Windows XP or Office 2003.
 - Ensure that your security vendors will continue to support Windows XP until the date you expect to have it eliminated.
 - Install a modern, supported browser to be used whenever possible.

- These solutions require time and money to implement (in order of preference):
 - Subscribe to Custom Support from Microsoft.
 - Remove the user's rights to the desktop (lockdown).
 - Implement application controls (limit the applications that can be used to those that are known).
 - Prevent configuration drift from known-good configurations.
 - Replace Windows XP with thin clients.
 - Segregate Windows XP machines on a separate network.

If there's not enough money to finish (do as many of these as practical):

- Ensure that your security vendors will continue to support Windows XP until the date you expect to have it eliminated.
- Revisit the business case to understand the cost and risk of remaining on Windows XP or Office 2003.
- Install a modern, supported browser to be used whenever possible.
- These solutions require time and money to implement (in order of preference):
 - Remove the user's rights to the desktop (lockdown).
 - Implement application controls (limit the applications that can be used to those that are known).
 - Prevent configuration drift from known-good configurations.
 - Segregate Windows XP machines on a separate network.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How to Protect Your PCs If You Are Still Running Windows XP in April 2014"

"Custom Support Will Be Available for Windows XP at a Price"

GARTNER HEADQUARTERS**Corporate Headquarters**

56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters

AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit <http://www.gartner.com/technology/about.jsp>

© 2013 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.